Operational Policy

Policy Title:	**Report and Response to Privacy and Security Incidents**		
Policy Number:	OHA-100-014		
Original Date:	7/22/2014	**Last Update:**	10/03/2016
Approved:	Mark Fairbanks, OHA CFO		

Purpose

This policy is one of a series that describes Oregon Health Authority (OHA) privacy and security guidelines and expectations for the necessary collection, storage, protection, use, and disclosure of confidential information about individuals in order to provide services and benefits to individuals, while maintaining reasonable safeguards to protect the privacy of information.

Description

This policy describes the responsibility of OHA staff to report known or suspected breaches of privacy or security; the rights of an individual to file complaints related to known or suspected breaches of privacy and security; and presents an overview of the responsibilities of the agency related to investigation and reporting of breaches.

Applicability

This policy applies to all OHA staff including employees, volunteers, interns and agency contractors.

As keepers of the public trust, all agency employees have a responsibility to comply with state and agency policies, administrative rule, and state and federal law. The agency takes this responsibility seriously and failure to fulfill this responsibility is not treated lightly. Employees who fail to comply with state or agency policy, administrative rule, or state and federal law may face progressive discipline, up to and including dismissal from state service.

Policy

1. All members of the OHA workforce have a duty to report privacy or security incidents and can do so without fear of retaliation.
2. A privacy incident is an allegation that an individual's protected information has been impermissibly acquired, accessed, used, disclosed, modified or destroyed through an information or security breach. The breach may be due to human error, access to or interference with information systems or assets.
3. A security incident is an allegation that information systems or assets, including computers, databases, servers or mobile media have been impermissibly accessed by unauthorized persons or authorized persons acting with malicious intent. The breach may be due to human error, access to or interference with information systems or assets.

4. When a member of the OHA workforce observes a privacy or security incident happening, the employee shall take any immediate corrective action that is appropriate to the time and location.
5. Within 24 hours of discovering a privacy or security incident, OHA workforce members shall use form MSC 3001 to report to the Information Security and Privacy Office (ISPO) any:
    a. Privacy or security complaints made by an individual, including those related to HIPAA.
    b. Suspected or known privacy or security incidents relating to an individual's identifiable or protected information.
    c. Suspected or known privacy or security incidents related to the violation of OHA policies and procedures that protect the privacy, security or confidentiality of an individual's protected information.
6. An incident is considered discovered on the first day an OHA workforce member or agent knows or if by exercising reasonable diligence would have known that the incident was occurring.
7. Individuals who think that OHA has failed to comply with federal and state statute and rule, including the HIPAA Privacy Rule or agency privacy and security policies and procedures may file a complaint with OHA Privacy Office or the Department of Health and Human Services (DHHS) Office of Civil Rights.
8. When a complaint or incident report is received by the Privacy Office, OHA shall:
    a. Work with the program to correct the incident to the extent practicable, as soon as possible and in no case more than 30 calendar days after the discovery.
    b. Complete a risk assessment to determine the probability that protected health information (PHI) has been acquired, accessed, used or disclosed, as soon as possible, and in no case more than 30 calendar days from the discovery,
    c. Mitigate, to the extent practicable, any known cause of the breach,
    d. Document all incidents and complaints and their resulting dispositions.
9. In accordance with HIPAA regulations and OHA policy, when ISPO determines that a breach has occurred and PHI may have been acquired, accessed, used or disclosed without appropriate authorization, the responsible OHA program, in consultation with the Privacy Office shall:
    a. Provide written notice of the breach to the affected individual or individuals no more than 60 days after the discovery of the breach; and
    b. Provide ISPO with documentation that notice has been provided.
10. The written notice shall be in plain language and shall:
    a. Be sent by first-class mail addressed to the affected individuals last known address, unless the individual has previously agreed to receive electronic notice.
    b. Contain the following information:
        i. A brief description of the incident;
        ii. A description of the types of PHI involved in the breach;
        iii. Any steps the individual should take to protect him or herself from harm that could result from the breach;
        iv. A brief description of the steps OHA is taking to review the breach, mitigate harm to the individual, and protect against future occurrences; and
        v. Contact information, including a toll-free telephone number, email address, website, or postal address for the individual to ask questions or obtain additional information.
11. If the written notice can't be provided because of insufficient contact information, OHA shall provide secondary notice in a way reasonably calculated to reach individuals whose information may be included in the breach.
12. If notice can't be provided to 10 or more individuals, the secondary notice form shall include a toll free number that remains active for at least 90 days and allows individuals to determine if their protected information was included in the breach.
13. If OHA determines there is the potential for imminent misuse of protected information in connection with an incident, OHA may provide information to individuals by telephone or other means, as appropriate, in addition to providing the required written notice as described above.

14. OHA shall notify DHHS of the privacy or security breach in accordance with HIPAA and other federal and state statute and rule and OHA policy.
    a. OHA considers any reports generated in response to a complaint to be prepared in anticipation of litigation. These records are not:
        i. Discoverable.
        ii. Part of the individual's record of client or patient care.
15. If OHA policy conflicts with federal or state statute or rule, that statute or rule supersedes unless the OHA policy provides more protection.

References

45 CFR 160 & 164
OAR 125-055-0100 to 125-055-0130
Privacy/Security Glossary of Common Terms

Contacts

Information Security and Privacy Office (ISPO)
Phone: 503-945-6812 (Security)
503-945-5780 (Privacy)
Fax: 503-947-5396
dhsinfo.security@state.or.us
dhs.privacyhelp@state.or.us

U. S. Department of Health and Human Services, Office for Civil Rights
Medical Privacy, Complaint Division
200 Independence Avenue, SW
Washington, D.C. 20201
Toll free Phone: 877-696-6775
Phone: 866-627-7748
TTY: 886-788-4989
Email: mailto:OCRComplaint@hhs.gov

Policy History
Version 1 Established 7/22/2014
Reviewed 10/03/2016

To request this policy in another format or language, contact the Publications and Design Section at 503-378-3486, 711 for TTY, or email dhs-oha.publicationrequest@state.or.us

Keywords
Individual privacy, Protecting privacy, Release of information, Releasing information, Breach, Reporting, Incident, Privacy Incident, Privacy and Security Incident